Information and Computation 209 (2011) 1007–1015

Contents lists available at ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

An ID-based multi-signer universal designated multi-verifier signature scheme

Ting-Yi Chang

Graduate Institute of e-Learning, National Changhua University of Education, No. 1, Jin-De Road, 500 Changhua City, Taiwan, ROC

ARTICLE INFO

Article history:
Received 19 April 2010
Revised 22 February 2011
Available online 7 April 2011

Keywords:
Bilinear pairing
Bilinear Diffie–Hellman problem
Identity-based cryptography
Multi-user setting
Universal designated verifier signature

ABSTRACT

In an ID-based universal designated verifier signature scheme, a single signer generates a signature that can only be verified by a designated verifier using a simplified public identity such as an e-mail address. In this paper, we expand the scheme to a multi-user setting for generating and verifying signatures in practical applications. An ID-based multi-signer universal designated multi-verifier signature scheme based on bilinear pairings is proposed that allows a set of multi-signer to cooperatively generate a signature and designate a set of multi-verifier to verify it. The security of the proposed scheme is demonstrated to be resistant to existentially forgery from adaptive chosen-message and chosen-ID attacks under the Bilinear Diffie–Hellman problem.

1. Introduction

Paperwork is rapidly being replaced as e-mail, electronic commerce, and electronic monetary transactions become more widespread. For many of these new forms of communication, a digital signature is essential. In traditional signature schemes such as RSA [1] and DSA [2], anyone can verify the validity of a signature by using the signer's public key, and the signer cannot successfully claim he/she did not sign a message. In numerous applications such as tenders, electronic voting, or electronic auctions, the public verification and non-repudiation properties of a signature are not desired. For an example, in electronic voting schemes, a voting center seeks to verify that a vote has been properly counted in the final tally by means of the center's signature on the receipt. Voters must not have the ability to use such receipts to verify the nature of their votes. Otherwise, it results that the briber believe that the voter indeed votes some candidate according to his/her direction and then give the obedient voter some gain.

To satisfy the above requirements in electronic voting schemes, the *designated verifier signature* (DVS) concept was introduced by Jakobsson, Sako, and Impagliazzo [3]. The signature of a message in the DVS scheme is intended to be a special verifier chosen by the signer, and only the designated verifier is able to verify its validity. This can be viewed as a "light signature scheme" [4]. No one else than the designated verifier can be convinced of the authenticity of this signature since the designated verifier himself can simulate the signature which is indistinguishable from the one generated by the signer. That is, no one can affirm the identity of the signer or the designated verifier who issued the signature. Jakobsson et al. also introduced a stronger vision of the DVS scheme called *strong designated verifier signature* (SDVS). In a SDVS scheme, the designated verifier's private key is involved in the verification phase so that no one else other than the designated verifier can verify the validity of signature. Later, Saeednia et al. [5] formalized SDVS notation and proposed an efficient scheme.

Steinfeld et al. [6] in Asiacrypt 2003 defined and proposed a new type of DVS scheme called an *universal designated verifier signature* (UDVS). It has the same properties as DVS schemes and it also can function as a standard publicly verifiable signature scheme that additionally allows any signature holder (not necessarily the signer) to designate the signature to any

E-mail address: tychang@cc.ncue.edu.tw.

0890-5401/$ – see front matter
doi:10.1016/j.ic.2011.03.002

desired designated verifier (using the verifier's public key). The security of their scheme is based on the Bilinear Diffie–Hellman (BDH) problem. Simultaneously, they demonstrated how to extend the classical Schnorr or RSA signature schemes to UDVS schemes [7]. Like SDVS schemes, the designated verifier's private key in the UDVS schemes is also involved in the verification phase. This is because the verifier's public key is used in the designated signature generation phase. However, the SDVS scheme is specially designed for designated verifier signatures, and does not provide an additional function to convert a publicly verifiable signature scheme into a designated verifier signature.

Some fair distributed contract signing and verifying schemes have been designed for use in a multi-user setting. For multi-verifier settings, Laguillaumie and Vergnaud [8,9] extended DVS notation and developed *designated multi-verifier signature* (DV$^{\mathrm{M}}$S). It differs from DVS in that the designated signature is intended to correspond to a specific set of different verifiers. On the other hand, Ng et al. [10] extended UDVS notation as *universal designated multi-verifier signature* (UDV$^{\mathrm{M}}$S) to allow a signature holder to designate the signature to multi-verifier. They proposed two UDV$^{\mathrm{M}}$S schemes based on Steinfeld et al.'s UDVS scheme. Shailaja et al. [11] and Yang et al. [12] proposed a UDV$^{\mathrm{M}}$S scheme based on the q-Strong Diffie–Hellman assumption and Gap Bilinear Diffie–Hellman assumption, respectively. The security of their schemes is proven in the standard model. For multi-signer settings, Zhang et al. [13] proposed a *multi-signer strong designated signature* (S$^{\mathrm{M}}$SDVS) based on the BDH assumption. The designated signature should be collectively generated by multi-signer and with no one able to verify its validity except the designated verifier. We refer to references [8–13] as providing examples of related work and applications for multi-user settings.

Most related designated verifier signature schemes are based on a certificate-based PKI (Public Key Infrastructure) [8–10, 5,7,11,6,12,13]. In certificate-based designated verifier signature schemes, a user must obtain a certificate of a long-lived public key from the CA (Certification Authority) and verify its correctness before utilizing the user's public key. Such certificate-based designated verifier signature schemes lead to the problems of certificate management and the high computational cost of certificate verification. In ID-based systems [14–18], a user's public key is derived from the identity such as email addresses, IP address and there is a trusted party KGC (Key Generation Center) that generates the corresponding private key of the user. Advantageous aspects of an ID-based system include not requiring the public key directories and simplified key revocation. Therefore, some ID-based designated verifier signature schemes have been proposed, such as *ID-based universal designated verifier signature* (ID-UDVS) [19], *ID-based strong designated verifier signature* (ID-SDVS) [20–22], and *ID-based universal designated multi-verifier signature* (ID-UDV$^{\mathrm{M}}$S) [23].

A designated signature scheme has not yet been developed for both multi-signer settings and multi-verifier settings. We expand the example presented in [13] to conform to these factors. A group of witnesses want to collectively report an offence to a prosecutor. To avoid retaliation, a multi-signer designated verifier signature can be used on the on the report allowing only a designated prosecutor to verify the signature. However, to avoid a briber to canvass a corrupt prosecutor is necessary. This can be accomplished by distributing the power of verifying a signature in a multi-verifier setting. That is, a multi-witness designated verifier signature on the report can only be verified by multi-prosecutors. A multi-user setting in the designated signature scheme would be best implemented by ID-based systems since more users' public keys are involved and used. Moreover, if the scheme has the property "universal," it will be more convenient than strong designated verifier signature schemes.

In this paper, an *ID-based multi-signer universal designated multi-verifier signature* (ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S) scheme is proposed, which generalizes an ID-UDVS scheme. In the ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S scheme, all users' public keys are derived from their identities simplifying the key management procedures. A publicly verifiable signature is cooperatively generated by multi-signer and any holder of the signature can designate it to any desired multi-verifier by using the verifiers' public keys. Given the designated signature, the designated multi-verifier can cooperatively verify that the message is signed by the multi-signer but cannot prove the same fact to a third party. Note that Lipmma et al. [24] identified a new security property for designated verifier signatures: the non-delegatability. This means that neither the signer or nor the designated verifier should able to produce a "meta-key" which allows to generate a new signature without revealing their secret keys. However, the delegatability is inherent to all related UDVS [25]. Since the proposed ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S is universal and belongs to UDVS, our scheme is delegatable. Regardless the numbers of signers and verifiers are, the generated signature length of the proposed ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S scheme is independent of the number of signers and verifiers. The proposed ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S scheme is secure against existential forgery under the chosen-message attacks and chosen-ID attacks in the random oracle model assuming the BDH problem is hard.

The remainder of this paper is organized as follows. Some basic concepts on bilinear pairing are introduced in Section 2. In Section 3, an ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S scheme is presented. Section 4 analyzes the security of the proposed ID-S$^{\mathrm{M}}$UDV$^{\mathrm{M}}$S scheme. The performance of the proposed scheme is presented in Section 5. Finally, Section 6 concludes the paper.

2. Preliminaries

2.1. Admissible bilinear pairings

Let $\mathbb{G}_1$ be a cyclic additive group and $\mathbb{G}_2$ be a cyclic multiplicative group of the same order q for some large prime q. An admissible bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, which satisfies the following properties:

- Bilinear: A map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is bilinear if $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$. This can also be stated as $e(P + Q, T) = e(P, T)e(Q, T)$ and $e(P, Q + T) = e(P, Q)e(P, T)$ for all $P, Q, T \in \mathbb{G}_1$.
- Non-degenerate: There exist $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.
- Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$.

2.2. Bilinear Diffie–Hellman assumption

The security of our scheme relies on the hardness of the Bilinear Diffie–Hellman problem.

Bilinear Diffie–Hellman parameter generator $\mathcal{G}$. A randomized algorithm $\mathcal{G}$ is a bilinear Diffie–Hellman parameter generator if (1) $\mathcal{G}$ takes a security parameter $\kappa \in \mathbb{Z}^+$, (2) $\mathcal{G}$ runs in polynomial time in κ, and (3) $\mathcal{G}$ outputs a κ-bit prime number q, the description of groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, and the description of an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$,

$$\mathcal{G}(1^\kappa) = \langle q, \mathbb{G}_1, \mathbb{G}_2, e \rangle.$$

Bilinear Diffie–Hellman (BDH) problem. Let $\mathcal{G}$ be a bilinear Diffie–Hellman parameter generator to generate $\langle q, \mathbb{G}_1, \mathbb{G}_2, e \rangle$. An algorithm $\mathcal{A}$ has advantage $\epsilon(\kappa)$ in solving the BDH problem for $\mathcal{G}$ and a random generator P of $\mathbb{G}_1$ if for sufficiently large κ:

$$Adv_{\mathcal{G},\mathcal{A}}(\kappa) = \Pr\left[\mathcal{A}(q, \mathbb{G}_1, \mathbb{G}_2, e, P, aP, bP, cP) = e(P, P)^{abc}\right] \geqslant \epsilon(\kappa),$$

where the probability is over the random choice of $a, b, c \in \mathbb{Z}_q^*$, $P \in \mathbb{G}_1$, and the random bits of $\mathcal{A}$. We say that $\mathcal{G}$ satisfies the BDH assumption if there is no randomized algorithm $\mathcal{A}$ that can solve the BDH problem with a non-negligible advantage $\epsilon(\kappa)$.

3. ID-based multi-signers universal designated multi-verifiers signature

In this section, we present an ID-based multi-signer universal designated multi-verifier signature (ID-S$^{\mathsf{M}}$UDV$^{\mathsf{M}}$S) scheme, which consists of eight algorithms: setup algorithm Setup, extract algorithm Extract, ID-based individual signature generation algorithm ID-S, ID-based individual signature public verification algorithm ID-SPV, ID-based multi-signer signature generation algorithm ID-S$^{\mathsf{M}}$, ID-based multi-signer signature public verification algorithm ID-S$^{\mathsf{M}}$PV, ID-based universal designated multi-verifier signature generation algorithm ID-UDV$^{\mathsf{M}}$, ID-based universal designated multi-verifier signature verification algorithm ID-UDV$^{\mathsf{M}}$V.

Setup: KGC runs BDH parameter generator $\mathcal{G}$ to generate a prime q, two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of order q, and an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. KGC chooses a random generator $P \in \mathbb{G}_1$, a random $s \in \mathbb{Z}_q^*$, and set $P_{pub} = sP$. Then, KGC keeps s as the master secret key and publishes system parameters $params = \langle q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_1, H_2 \rangle$, where $H_1 : \{0,1\}^* \to \mathbb{G}_1$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$ are cryptographic hash functions.

Extract: Given an identity ID, KGC computes the public key $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$ and the private key $S_{\mathrm{ID}} = sQ_{\mathrm{ID}}$, and returns S_{ID} to the user with identity ID.

ID-S: Let $\mathbf{S} = \{\mathrm{ID}_{Si},\ i = 1, \ldots, n\}$ be a set of signers' identities, each signer performs the following steps to generate his individual signature on a message m:

(1) Choose a random $r_i \in \mathbb{Z}_q^*$ to compute

$$U_i = r_i H_1(\mathrm{ID}_{Si}), \tag{1}$$

and then broadcast U_i to other co-signers.

(2) Compute

$$\overline{U} = \sum_{i=1}^{n} U_i, \tag{2}$$

$$h = H_2(m, \overline{U}), \tag{3}$$

$$V_i = (r_i + h)S_{\mathrm{ID}_{Si}}. \tag{4}$$

The ID-based individual signature (ID-S signature) on the message m is $\sigma_i = (U_i, V_i, \overline{U})$.

ID-SPV: Given the system parameters *params*, a message m, a ID-S signature $\sigma_i = (U_i, V_i, \overline{U})$, check if

$$e(V_i, P) \stackrel{?}{=} e\big(U_i + H_2(m, \overline{U})H_1(\mathrm{ID}_{Si}), P_{pub}\big). \tag{5}$$

If it holds, then the ID-S signature is valid and output accepted; otherwise, output is rejected.

ID-S^{M}: Combine n co-singers' ID-S signatures σ_is on the message m:

$$\overline{V} = \sum_{i=1}^{n} V_i. \tag{6}$$

The ID-based multi-signer signature (ID-S^{M} signature) on the message m is $\overline{\sigma} = (\overline{U}, \overline{V})$.

ID-S^{M}PV: Given the system parameter *params*, a message m, a ID-S^{M} signature $\overline{\sigma} = (\overline{U}, \overline{V})$, check if

$$e(\overline{V}, P) \stackrel{?}{=} e\left(\overline{U} + H_2(m, \overline{U})\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_i)\right), P_{pub}\right). \tag{7}$$

If it holds, then output accepted; otherwise, output rejected.

ID-UDV^{M}: Let $\mathbf{V} = \{\mathrm{ID}_{Vj},\ j = 1, \ldots, l\}$ be a set of verifiers' identities. Given a set $\mathbf{V}$ and a message-signature pair $(m, \overline{\sigma})$, compute

$$\overline{V}_{DV} = e\left(\overline{V}, \sum_{j=1}^{l} H_1(\mathrm{ID}_{Vj})\right). \tag{8}$$

The universal designated multi-verifier signature (ID-UDV^{M} signature) on the message m is $\overline{\sigma}_{DV} = (\overline{U}, \overline{V}_{DV})$. This algorithm ID-UDV^{M} functions the publicly verifiable multi-signer signature $\overline{\sigma} = (\overline{U}, \overline{V})$ to allow any holder of the signature can designate it to any multi-verifier.

ID-UDV^{M}V: Given a set $\mathbf{S}$ of signers' public keys, a set $\mathbf{V}$ of verifiers's private keys, and a message-signature pair $(m, \overline{\sigma}_{DV})$, check if

$$\overline{V}_{DV} \stackrel{?}{=} \prod_{j=1}^{l} e\left(\overline{U} + H_2(m, \overline{U})\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), S_{\mathrm{ID}_{Vj}}\right). \tag{9}$$

If it holds, then output accept; otherwise, output reject.

It can be seen that the lengths of the generated signatures in algorithms ID-S^{M} and ID-UDV^{M} are independent of the number of signers and verifiers. Next, we show the completeness of the ID-S^{M}UDV^{M}S scheme with regard to algorithms ID-SPV, ID-S^{M}PV, ID-UDV^{M}V.

Theorem 3.1. *In algorithm* ID-SPV, *the* ID-S *signature* $\sigma_i = (U_i, V_i, \overline{U})$ *on the message* m *can be verified using Eq.* (5).

Proof.

$$\begin{aligned}
e(V_i, P) &= e\big((r_i + h) S_{\mathrm{ID}_{Si}}, P\big) && \text{by Eq. (4)}\\
&= e\big((r_i + h) Q_{\mathrm{ID}_{Si}}, P_{pub}\big) && \text{by bilinear property}\\
&= e\big(r_i H_1(\mathrm{ID}_{Si}) + h H_1(\mathrm{ID}_{Si}), P_{pub}\big)\\
&= e\big(U_i + H_2(m, \overline{U}) H_2(\mathrm{ID}_{Si}), P_{pub}\big) && \text{by Eq. (1).} \quad \square
\end{aligned}$$

Theorem 3.2. *In algorithm* ID-S^{M}PV, *the* ID-S^{M} *signature* $\overline{\sigma} = (\overline{U}, \overline{V})$ *on the message* m *can be verified using Eq.* (7).

Proof.

$$\begin{aligned}
e(\overline{V}, P) &= e\left(\sum_{i=1}^{n} V_i, P\right) && \text{by Eq.(6)}\\
&= e\left(\sum_{i=1}^{n} (r_i + h) S_{\mathrm{ID}_{Si}}, P\right) && \text{by Eq. (4)}\\
&= e\left(\sum_{i=1}^{n} (r_i + h) Q_{\mathrm{ID}_{Si}}, P_{pub}\right) && \text{by bilinear property}\\
&= e\left(\sum_{i=1}^{n} r_i H_1(\mathrm{ID}_{Si}) + h \sum_{i=1}^{n} H_1(\mathrm{ID}_{Si}), P_{pub}\right)\\
&= e\left(\overline{U} + h \sum_{i=1}^{n} H_1(\mathrm{ID}_{Si}), P_{pub}\right) && \text{by Eq. (2).} \quad \square
\end{aligned}$$

Theorem 3.3. *In algorithm* ID-UDV^{M}V, *the* ID-S^{M} *signature* $\overline{\sigma}_{DV} = (\overline{U}, \overline{V}_{DV})$ *on the message m can be verified using Eq.* (9).

Proof.

$$\begin{aligned}
\overline{V}_{DV} &= e\left(\overline{V}, \sum_{j=1}^{l} H_1(\mathrm{ID}_{\mathrm{V}j})\right) && \text{by Eq. (8)}\\
&= \prod_{j=1}^{l} e\big(\overline{V}, H_1(\mathrm{ID}_{\mathrm{V}j})\big) && \text{by bilinear property}\\
&= \prod_{j=1}^{l} e\left(\sum_{i=1}^{n}(r_i + h) S_{\mathrm{ID}_{\mathrm{S}i}}, H_1(\mathrm{ID}_{\mathrm{V}j})\right) && \text{by Eqs. (4), (6)}\\
&= \prod_{j=1}^{l} e\left(\sum_{i=1}^{n}(r_i + h) H_1(\mathrm{ID}_{\mathrm{S}i}), S_{\mathrm{ID}_{\mathrm{V}j}}\right) && \text{by bilinear property}\\
&= \prod_{j=1}^{l} e\left(\overline{U} + H_2(m, \overline{U})\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{\mathrm{S}i})\right), S_{\mathrm{ID}_{\mathrm{V}j}}\right) && \text{by Eq. (1) and Eq. (2).} \quad \square
\end{aligned}$$

4. Security analysis

The ID-S signatures are secure has been proved by Lin et al. [26], which is equivalent to the signature in Cha–Cheon scheme [27] under the assumption of a one-way hash function H_1. For the message m, combining n ID-S signatures $\sigma_i = (U_i, V_i, \overline{U})$ into a ID-S^{M} signature $\overline{\sigma} = (\overline{U}, \overline{V})$, is the same as the Cha–Cheon signature if the public key Q_{ID} is treated as: $\sum_{i=1}^{n} H_1(\mathrm{ID}_{\mathrm{S}i})$. Their scheme has been proved secure against existential forgery under the chosen-message attacks and chosen-ID attacks in the random oracle model assuming the BDH problem is hard in groups generated by $\mathcal{G}$. Due to limitations of space, in this paper we omit the detailed descriptions of those proofs here. We directly prove the unforgeability and non-transferability of ID-S^{M}UDV^{M}S as follows.

Theorem 4.1 *(Unforgeability). In the random oracle model, the proposed ID-based multi-signer universal designated multi-verifier signature scheme* ID-S^{M}UDV^{M}S = (Setup, Extract, ID-S, ID-SPV, ID-S^{M}, ID-S^{M}PV, ID-UDV^{M}, ID-UDV^{M}V) *is existentially unforgeable against an adaptively chosen-message and chosen-ID attacker under the BDH assumption. Concretely, suppose there exists an adversary* $\mathcal{A}$ *who has an advantage* $\epsilon_{\mathcal{A}}(\kappa)$ *in attacking* ID-S^{M}UDV^{M}S. *Then there exists an algorithm* $\mathcal{B}$ *that solves the BDH problem generated by* $\mathcal{G}$ *with an advantage* $\epsilon_{\mathcal{B}}(\kappa)$ *at least*:

$$\epsilon_{\mathcal{B}}(\kappa) \geqslant \epsilon_{\mathcal{A}}(\kappa) \cdot \frac{2}{q_{H_1}(q_{H_1} - 1)}.$$

Proof. Algorithm $\mathcal{B}$ is given as inputting the BDH parameters $\langle q, \mathbb{G}_1, \mathbb{G}_2, e\rangle$ generated by $\mathcal{G}$ and a random instance $\langle P, aP, bP, cP\rangle$ of the BDH problem for these parameters. $\mathcal{B}$ is to inject the above $\langle P, aP, bP, cP\rangle$ during the simulation, and to compute $e(P, P)^{abc}$.

- Setup: $\mathcal{B}$ creates the ID-S^{M}UDV^{M}S parameters $params = \langle q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_{pub}, H_1, H_2\rangle$ by setting $P_{pub} = aP$. Here H_1, H_2 are two random oracles controlled by $\mathcal{B}$. To avoid collision and consistently respond to hash queries, $\mathcal{B}$ maintains two lists $list_{H_1}$ and $list_{H_2}$ which are initially empty. $\mathcal{B}$ returns the same output for identical inputs in hash queries. That is, $\mathcal{B}$ first checks the existence before creating a new output.
- $\mathsf{H}_1(\mathrm{ID}_i)$: Assume $\mathcal{A}$ makes at most q_{H_1} distinct queries to H_1, $\mathcal{B}$ then chooses $j, k \in [1, q_{H_1}]$ uniformly at random. When $\mathcal{A}$ makes an $\mathsf{H}_1(\mathrm{ID}_i)$ query, $\mathcal{B}$ maintains $list_{H_1}$ as follows:
  - If $i = j$, let $\mathrm{ID}^*_{\mathrm{S}} = \mathrm{ID}_i$ at this point. $\mathcal{B}$ returns bP and adds $\langle \mathrm{ID}^*_{\mathrm{S}}, \perp, bP\rangle$ to $list_{H_1}$.
  - If $i = k$, let $\mathrm{ID}^*_{\mathrm{V}} = \mathrm{ID}_i$ at this point. $\mathcal{B}$ returns cP and adds $\langle \mathrm{ID}^*_{\mathrm{V}}, \perp, cP\rangle$ to $list_{H_1}$.
  - Otherwise, $\mathcal{B}$ picks a random $t_i \in \mathbb{Z}^*_q$ and returns $t_i P$, and add $\langle \mathrm{ID}_i, t_i, t_i P\rangle$ to $list_{H_1}$.
- $\mathsf{H}_2(m_i, \overline{U}_i)$: When $\mathcal{A}$ makes an $\mathsf{H}_2(m_i, \overline{U}_i)$ query, $\mathcal{B}$ picks a random $h_i \in \mathbb{Z}^*_q$, returns h_i, and adds $\langle m_i, \overline{U}_i, h_i\rangle$ to $list_{H_2}$.
- Extract(ID_i): When $\mathcal{A}$ makes an Extract(ID_i) query, if $\mathrm{ID}_i \neq \mathrm{ID}^*_{\mathrm{S}}$ and $\mathrm{ID}_i \neq \mathrm{ID}^*_{\mathrm{V}}$, $\mathcal{B}$ finds the tuple of the form $\langle \mathrm{ID}_i, t_i, t_i P\rangle$ and returns $t_i aP$. Otherwise $\mathcal{B}$ reports failure and terminates. It is reasonable to assume that $\mathcal{A}$ asked for $\mathsf{H}_1(\mathrm{ID}_i)$ before issuing Extract(ID_i) queries.
- ID-S^{M}($\mathbf{S}_i, m_i$): When $\mathcal{A}$ makes an ID-S^{M}($\mathbf{S}_i, m_i$) query of a set of identities $\mathbf{S}_i$ and a message m_i, $\mathcal{B}$ returns a ID-S^{M} signature $\overline{\sigma}_i = (\overline{U}_i, \overline{V}_i)$ as follows. First, $\mathcal{B}$ chooses a random $h_i \in \mathbb{Z}^*_q$ for an ID-S^{M}($\mathbf{S}_i, m_i$) query. For each ID_α in $\mathbf{S}_i$, $\mathcal{B}$ chooses a random $r_\alpha \in \mathbb{Z}^*_q$.
  - If $\mathrm{ID}_\alpha \neq \mathrm{ID}^*_{\mathrm{S}}$ and $\mathrm{ID}_\alpha \neq \mathrm{ID}^*_{\mathrm{V}}$, $\mathcal{B}$ finds the tuples of the form $\langle \mathrm{ID}_\alpha, t_\alpha, t_\alpha P\rangle$ in $list_{H_1}$, and then computes $U_\alpha = r_\alpha t_\alpha P$, $V_\alpha = (r_\alpha + h_i) t_\alpha aP$.

– If $\mathrm{ID}_\alpha = \mathrm{ID}_S^*$, $\mathcal{B}$ computes $U_\alpha = r_\alpha P - h_i bP$, $V_\alpha = r_\alpha aP$.
– If $\mathrm{ID}_\alpha = \mathrm{ID}_V^*$, $\mathcal{B}$ computes $U_\alpha = r_\alpha P - h_i cP$, $V_\alpha = r_\alpha aP$.

Then, $\mathcal{B}$ combines ID-S signatures to a ID-S$^{\mathsf{M}}$ signature $\overline{\sigma}_i = (\overline{U}_i, \overline{V}_i)$, where $\overline{U}_i = \sum_{\mathrm{ID}_\alpha \in \mathbf{S}_i} U_\alpha$ and $\overline{V}_i = \sum_{\mathrm{ID}_\alpha \in \mathbf{S}_i} V_\alpha$. Finally, $\mathcal{B}$ returns $\overline{\sigma}_i = (\overline{U}_i, \overline{V}_i)$ and adds $\langle m_i, \overline{U}_i, h_i \rangle$ to $list_{H_2}$.

Eventually, $\mathcal{A}$ outputs a valid ID-UDV$^{\mathsf{M}}$ signature $(\mathbf{S}_t = \{\mathrm{ID}_{S1}, \ldots, \mathrm{ID}_{Sn}\}_t, \mathbf{V}_t = \{\mathrm{ID}_{V1}, \ldots, \mathrm{ID}_{Vl}\}_t, m_t, \overline{\sigma}_{DV_t})$ where $\mathbf{S}_t$ and $\mathbf{V}_t$ are the sets of identities to be selected by $\mathcal{A}$. If $\mathrm{ID}_{Si} \neq \mathrm{ID}_S^* \in \mathbf{S}_t$ and $\mathrm{ID}_{Vi} \neq \mathrm{ID}_V^* \in \mathbf{V}_t$, $\mathcal{B}$ reports failure and terminates. Otherwise by replaying of $\mathcal{B}$ with the same random type but different choice of a random set for H_2-queries. As in the forking lemma argument of [28], $\mathcal{B}$ gets two ID-UDV$^{\mathsf{M}}$ signatures $(\mathbf{S}_t, \mathbf{V}_t, m_t, \overline{\sigma}_{DV_t})$ and $(\mathbf{S}_t, \mathbf{V}_t, m_t', \overline{\sigma}'_{DV_t})$ which are expected to be valid with respect to different $h \neq h'$, where $\overline{\sigma}_{DV_t} = (\overline{U}_t, \overline{V}_{DV_t})$, $\overline{V}_{DV_t} = e(\overline{V}_t, \sum_{\mathrm{ID}_{Vi} \in \mathbf{V}_t} Q_{\mathrm{ID}_{Vi}})$, $\overline{\sigma}'_{DV_t} = (\overline{U}_t, \overline{V}'_{DV_t})$, $\overline{V}'_{DV_t} = e(\overline{V}'_t, \sum_{\mathrm{ID}_{Vi} \in \mathbf{V}_t} Q_{\mathrm{ID}_{Vi}})$. $\mathcal{B}$ computes the following equations to get $e(P,P)^{abc}$:

$$\frac{\overline{V}_{DV_t}}{e(\overline{U}_t + h\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t} Q_{\mathrm{ID}_{Si}}, \sum_{\mathrm{ID}_{Vi} \in \mathbf{V}_t, \mathrm{ID}_{Vi} \neq \mathrm{ID}_V^*} S_{\mathrm{ID}_{Vi}})} = e(\overline{V}_t, Q_{\mathrm{ID}_V^*}),$$

$$\frac{\overline{V}'_{DV_t}}{e(\overline{U}_t + h'\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t} Q_{\mathrm{ID}_{Si}}, \sum_{\mathrm{ID}_{Vi} \in \mathbf{V}_t, \mathrm{ID}_{Vi} \neq \mathrm{ID}_V^*} S_{\mathrm{ID}_{Vi}})} = e\big(\overline{V}'_t, Q_{\mathrm{ID}_V^*}\big),$$

$$\left(\frac{e(\overline{V}_t, Q_{\mathrm{ID}_V^*})}{e(\overline{V}'_t, Q_{\mathrm{ID}_V^*})}\right)^{(h-h')^{-1}} = e\left(\big(h-h'\big)\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t} S_{\mathrm{ID}_{Si}}, Q_{\mathrm{ID}_V^*}\right)^{(h-h')^{-1}} = e\left(\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t} S_{\mathrm{ID}_{Si}}, Q_{\mathrm{ID}_V^*}\right),$$

$$\frac{e(\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t} S_{\mathrm{ID}_{Si}}, Q_{\mathrm{ID}_V^*})}{e(\sum_{\mathrm{ID}_{Si} \in \mathbf{S}_t, \mathrm{ID}_{Si} \neq \mathrm{ID}_S^*} S_{\mathrm{ID}_{Si}}, Q_{\mathrm{ID}_V^*})} = e(S_{\mathrm{ID}_S^*}, Q_{\mathrm{ID}_V^*}) = e(abP, cP) = e(P,P)^{abc}.$$

If algorithm $\mathcal{B}$ does not abort during the simulation then algorithm $\mathcal{A}$'s view is identical to its view in the real attack. The responses to H_1-queries and H_2-queries are as in the real attack, since each response is uniformly and independently distributed in $\mathbb{G}_1$ and $\mathbb{Z}_q^*$ respectively. The responses to Extract-queries are valid since $t_i aP = aQ_{\mathrm{ID}_i} = S_{\mathrm{ID}_i}$. The responses $\overline{\sigma}_i = (\overline{U}_i, \overline{V}_i)$ to ID-S$^{\mathsf{M}}$-queries are valid, which can pass the verification equation (7). Obviously, if all identities in $\mathbf{S}_i$ such that $\mathrm{ID}_\alpha \neq \mathrm{ID}_S^*$ and $\mathrm{ID}_\alpha \neq \mathrm{ID}_V^*$, $\mathcal{B}$ knows the corresponding secret key t_α, and computes the values U_α and V_α following Eq. (1) and Eq. (4) respectively. It is obvious that the combined values $\overline{U}_i$ and $\overline{V}_i$ can pass the verification equation. If one of identities in $\mathbf{S}_i$ such that $\mathrm{ID}_\alpha = \mathrm{ID}_S^*$, i.e., $\mathbf{S}_i = \{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n\}_i$, $\mathrm{ID}_1 = \mathrm{ID}_S^*, \mathrm{ID}_2 \neq \mathrm{ID}_S^*, \ldots, \mathrm{ID}_n \neq \mathrm{ID}_S^*$. The combined values $\overline{U}_i = r_1 P - h_i bP + r_2 t_2 P + \cdots + r_n t_n P$ and $\overline{V}_i = r_1 aP + (r_2 + h_i)t_2 aP + \cdots + (r_n + h_i)t_n aP$ still can pass Eq. (7) as follows.

$$\begin{aligned}
e(\overline{V}_i, P) &= e\big(r_1 aP + (r_2 + h_i)t_2 aP + \cdots + (r_n + h_i)t_n aP, P\big) \\
&= e\big(r_1 P + (r_2 + h_i)t_2 P + \cdots + (r_n + h_i)t_n P, P_{pub}\big) \\
&= e\big(r_1 P + r_2 t_2 P + \cdots + r_n t_n P + h_i(t_2 P + \cdots + t_n P), P_{pub}\big) \\
&= e\big(\overline{U}_i + h_i bP + h_i(t_2 P + \cdots + t_n P), P_{pub}\big) \\
&= e\big(\overline{U} + h_i\big(H_1(\mathrm{ID}_1) + \cdots + H_1(\mathrm{ID}_n)\big), P_{pub}\big).
\end{aligned}$$

For the same derivation, if one of the identities in $\mathbf{S}_i$ is such that $\mathrm{ID}_\alpha = \mathrm{ID}_V^*$, then the signature $\overline{\sigma}_i = (\overline{U}_i, \overline{V}_i)$ will pass the verification.

Now the probability that $\mathcal{B}$ does not abort during the simulation should be assessed. The number of identity pairs is:

$$\begin{aligned}
\binom{q_{H_1}}{2} &= \frac{q_{H_1}!}{2!(q_{H_1}-2)!}, \\
&= \frac{q_{H_1}(q_{H_1}-1)}{2}.
\end{aligned}$$

Among those $\frac{q_{H_1}(q_{H_1}-1)}{2}$ pairs, at least one pair $(\mathrm{ID}_S^*, \mathrm{ID}_V^*)$ of them will never be the subject of a key extraction query from $\mathcal{A}$. Then, with a probability greater than $\frac{2}{q_{H_1}(q_{H_1}-1)}$, $\mathcal{A}$ will not ask the queries Extract(ID_S^*) and Extract(ID_V^*). Clearly $\mathcal{B}$'s advantage $\epsilon_{\mathcal{B}}(\kappa)$ for solving the BDH problem is the product of $\mathcal{A}$'s advantage $\epsilon_{\mathcal{A}}(\kappa)$ and the probability that $\mathcal{A}$ asks Extract queries on $(\mathrm{ID}_S^*, \mathrm{ID}_V^*)$. Hence the advantage $\epsilon_{\mathcal{B}}(\kappa) \geqslant \epsilon_{\mathcal{A}}(\kappa) \cdot \frac{2}{q_{H_1}(q_{H_1}-1)}$. Therefore, if a forger breaks ID-S$^{\mathsf{M}}$UDV$^{\mathsf{M}}$S, then an attacker can solve the BDH problem. □

Theorem 4.2 *(Non-transferability). The proposed ID-based multi-signer universal designated multi-verifier signature scheme* ID-S$^{\mathsf{M}}$UDV$^{\mathsf{M}}$S *achieves the non-transferability (source hiding). That is, each designated verifier cannot convince anyone of the authenticity of the* ID-UDV$^{\mathsf{M}}$ *signature* $\overline{\sigma}_{DV} = (\overline{U}, \overline{V}_{DV})$ *on the message m, even if all private keys are revealed.*

Proof. Given a ID-UDV^{M} signature $\overline{\sigma}_{DV} = (\overline{U}, \overline{V}_{DV})$ on the message m, the designated multi-verifier $\mathbf{V} = \{\mathrm{ID}_{Vj},\ j = 1, \ldots, l\}$ can always produce a valid ID-UDV^{M} signature $\overline{\sigma}'_{DV} = (\overline{U}', \overline{V}'_{DV})$ on the message m as follows:

(1) Choose $r'_1, r'_2, \ldots, r'_n \in \mathbb{Z}_q^*$ at random and compute $\overline{U}' = \sum_{i=1}^{n} r'_i H_1(\mathrm{ID}_{Si})$.
(2) Each designated verifier computes

$$e_j = e\left(\overline{U}' + H_2\left(m, \overline{U}'\right)\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), S_{\mathrm{ID}_{Vj}}\right),$$

and

$$\overline{V}'_{DV} = \prod_{j=1}^{l} e\left(\overline{U}' + H_2\left(m, \overline{U}'\right)\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), S_{\mathrm{ID}_{Vj}}\right)$$

The ID-UDV^{M} signature $\overline{\sigma}'_{DV} = (\overline{U}', \overline{V}'_{DV})$ on the message m passes algorithm ID-UDV^{M}V:

$$\begin{aligned}
\overline{V}'_{DV} &= \prod_{j=1}^{l} e\left(\overline{U}' + H_2\left(m, \overline{U}'\right)\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), S_{\mathrm{ID}_{Vj}}\right) \\
&= e\left(\overline{U}' + H_2\left(m, \overline{U}'\right)\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), \sum_{j=1}^{l} S_{\mathrm{ID}_{Vj}}\right) \\
&= e\left(\sum_{i=1}^{n} r'_i H_1(\mathrm{ID}_{Si}) + H_2\left(m, \overline{U}'\right)\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), \sum_{j=1}^{l} S_{\mathrm{ID}_{Vj}}\right) \\
&= e\left(\sum_{i=1}^{n} r'_i S_{\mathrm{ID}_{Si}} + h'\left(\sum_{i=1}^{n} H_1(\mathrm{ID}_{Si})\right), \sum_{j=1}^{l} Q_{\mathrm{ID}_{Vj}}\right) \\
&= e\left(\overline{V}', \sum_{j=1}^{l} H_1(\mathrm{ID}_{Vj})\right).
\end{aligned}$$

So given a message m, the distribution of $\overline{\sigma}'_{DV} = (\overline{U}', \overline{V}'_{DV})$ is perfectly indistinguishable from that of $\overline{\sigma}_{DV} = (\overline{U}, \overline{V}_{DV})$. It is unconditionally infeasible to determine who the original signers **S** and the designated verifiers **V** generate this signature, even if all private keys are revealed. Thus, the proposed ID-S^{M}UDV^{M}S achieves non-transferability. □

5. Performance evaluation

The proposed ID-S^{M}UDV^{M}S scheme is a new model under multi-signer/multi-verifier settings that is different from other schemes. Obviously, the ID-S^{M}UDV^{M}S scheme is a generalized version of ID-based universal designated verifier signature schemes, which includes one singer/one verifier settings, one singer/multi-verifier settings, multi-signer/one verifier setting, and multi-signer/multi-verifier setting. For facilitating the performance evaluation of our scheme, we first define the following notations:

T_P	the time for computing one pairing operation.
T_{H_1}	the time for mapping an identity to an element in $\mathbb{G}_1$ (map-to-point operation) by H_1.
T_{H_2}	the time for computing a hash value in $\mathbb{Z}_q^*$ by H_2.
T_M	the time for computing one ordinary scalar multiplication in $\mathbb{G}_1$.
T_A	the time for computing point addition on $\mathbb{G}_1$.
T_{MM}	the time for computing one modular multiplication.
T_{MA}	the time for computing one modular addition.

The time for performing the modular addition, the point addition, and the modular multiplication is low as compared to that of those performing the above operations. Note that the computation of pairing operations is most time-consuming, and has no thing to do with the number of signers and the number of verifiers. Assume that the bit length in $\mathbb{G}_2$ is $|\mathbb{G}_2|$ and in q is $|q|$. The detailed evaluation of the proposed scheme with n signers and l verifiers is listed in Table 1. That is, the proposed scheme can be practically implemented.

Table 1
Computational costs and signature lengths for the proposed ID-S^{M}UDV^{M}S scheme.

Signature generation phase			
ID-S	ID-SPV	ID-S^{M}	ID-S^{M}PV
$2T_M + T_{H_1} + (n-1)T_A + T_{H_2} + T_{MA}$	$2T_P + T_A + T_{H_2} + T_M + T_{H_1}$	$(n-1)T_A$	$2T_P + nT_A + T_{H_2} + T_M + nT_{H_1}$
Signature verification phase			
ID-UDV^{M}	ID-UDV^{M}V		
$T_P + lT_{H_1} + (l-1)T_A$	$nT_A + T_{H_2} + T_M + nT_{H_1} + T_P + (l-1)T_{MM}$		
Signature lengths			
ID-S	ID-S^{M}	ID-UDV^{M}	
$3\|q\|$	$2\|q\|$	$\|q\| + \|\mathbb{G}_2\|$	

6. Conclusions

In this paper, we presented an ID-based multi-signer universal designated multi-verifier signature scheme that generalizes the basic ID-based universal designated verifier signature schemes for more applications. We employ the ID-based cryptography to simplify the key management procedures. Through the multi-user setting is in the scheme, the signature length is independent of the number of signers and verifiers. Concerning the BDH problem, this study has demonstrated that the proposed scheme is provably secure against existential forgery under the chosen-message attacks and chosen-ID attacks in the random oracle model.

Acknowledgments

I would like to thank the referees for many valuable comments and suggestions which have resulted in several improvements of the presentation of the paper. This research was partially supported by the National Science Council, Taiwan, ROC, under contract Nos. NSC99-2221-E-018-018 and NSC99-2221-E018-021.

References

[1] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[2] National Institute of Standards and Technology (NIST), The digital signature standard proposed by NIST, Commun. ACM 35 (7) (1992) 36–40.
[3] M. Jakobsson, K. Sako, R. Impagliazzo, Designated verifier proofs and their applications, in: Advances in Cryptology, Eurocrypt'96, in: Lecture Notes in Comput. Sci., vol. 1070, 1996, pp. 142–154.
[4] R. Rivest, A. Shamir, Y. Tauman, How to leak a secret, in: Advances in Cryptology, Asiacrypt'01, in: Lecture Notes in Comput. Sci., vol. 2248, 2001, pp. 552–565.
[5] S. Saeednia, S. Kremer, O. Markowitch, An efficient strong designated verifier signature scheme, in: Proceedings of ICISC'03, in: Lecture Notes in Comput. Sci., vol. 2869, 2003, pp. 40–54.
[6] R. Steinfeld, L. Bull, H. Wang, J. Piperzyk, Universal designated-verifier signatures, in: Advances in Cryptology, Asiacrypt'03, in: Lecture Notes in Comput. Sci., vol. 2894, 2003, pp. 523–543.
[7] R. Steinfeld, H. Wang, J. Pieprzyk, Efficient extension of standard schnorr/RSA signatures into universal designated-verifier signatures, in: Proceedings of PKC 2004, in: Lecture Notes in Comput. Sci., vol. 2947, 2004, pp. 86–100.
[8] F. Laguillaumie, D. Vergnaud, Multi-designated verifiers signatures, in: Proceedings of ICICS'04, in: Lecture Notes in Comput. Sci., vol. 3269, 2004, pp. 495–507.
[9] F. Laguillaumie, D. Vergnaud, Multi-designated verifiers signatures: Anonymity without encryption, Inform. Process. Lett. 102 (2-3) (2007) 127–132.
[10] C.Y. Ng, W. Susilo, Y. Mu, Universal designated multi verifiers signature schemes, in: Proceedings of ICPADS'05, 2005, pp. 305–309.
[11] G. Shailaja, K.P. Kumar, A. Saxenh, Universal designated multi verifier signature without random oracles, in: Proceedings of ICIT'06, 2006, pp. 168–171.
[12] M. Yang, W. Yumin, Universal designated multi verifier signature scheme without random oracles, Wuhan Univ. J. Nat. Sci. 13 (6) (2008) 685–691.
[13] Y. Zhang, J. Zhang, Y. Zhang, Multi-signers strong designated verifier signature scheme, in: Proceedings of SNPD'08, 2008, pp. 324–328.
[14] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: Advances in Cryptology, Crypto'01, in: Lecture Notes in Comput. Sci., vol. 2193, 2001, pp. 213–229.
[15] T.Y. Chang, An ID-based group-oriented decryption scheme secure against adaptive chosen-ciphertext attacks, Comput. Commun. 32 (17) (2009) 1829–1836.
[16] L. Chen, Z. Cheng, N.P. Smart, Identity-based key agreement protocols from pairings, Internat. J. Inf. Secur. 6 (4) (2007) 213–241.
[17] L. Harn, J. Ren, C. Li, Efficient identity-based GQ multisignatures, Intern. J. Inf. Secur. 8 (3) (2009) 205–210.
[18] A. Shamir, Identity-based cryptosystems and signature schemes, in: Advances in Cryptology, Crypto'84, in: Lecture Notes in Comput. Sci., vol. 196, 1984, pp. 47–53.
[19] F. Zhang, W. Susilo, Y. Mu, X. Chen, Identity-based universal designated verifier signatures, in: Proceedings of SecUbiq 2005, in: Lecture Notes in Comput. Sci., vol. 3823, 2005, pp. 825–834.
[20] P.K. Kancharla, S. Gummadidala, Identity based strong designated verifier signature scheme, Informatica 18 (2) (2007) 239–252.
[21] B. Kang, C. Boyd, E. Dawson, A novel identity-based strong designated verifier signature scheme, J. Syst. Softw. 82 (2) (2009) 270–273.
[22] W. Susilo, F. Zhang, Y. Mu, Identity-based strong designated verifier signature schemes, in: Proceedings of ACISP'04, in: Lecture Notes in Comput. Sci., vol. 3108, 2004, pp. 313–324.
[23] S.H. Seo, J.Y. Hwang, K.Y. Choi, D.H. Lee, Identity-based universal designated multi-verifiers signature schemes, Comput. Standards & Interfaces 30 (5) (2008) 288–295.
[24] H. Lipmaa, G. Wang, F. Bao, Designated verifier signature schemes: Attacks, new security notions and a new construct, in: Proceedings of ICALP'05, in: Lecture Notes in Comput. Sci., vol. 3580, 2005, pp. 459–471.

[25] F. Laguillaumie, B. Libert, J.J. Quisquater, Universal designated verifier signatures without random oracles or non-black box assumptions, in: Fifth Conference on Security and Cryptography for Networks, SCN 06, in: Lecture Notes in Comput. Sci., vol. 4116, 2006, pp. 63–77.
[26] C.Y. Lin, T.C. Wu, F. Zhang, J.J. Hwang, New identity-based society oriented signature schemes from pairings on elliptic curves, Appl. Math. Comput. 160 (1) (2005) 245–260.
[27] J.C. Cha, J.H. Cheon, An identity-based signature from gap Diffie–Hellman groups, in: Proceeding of PKC 2003, in: Lecture Notes in Comput. Sci., vol. 2567, 2003, pp. 18–30.
[28] D. Pointcheval, J. Stern, Security arguments for digital signatures and blind signatures, J. Cryptology 13 (3) (2000) 361–396.